**What if Security Culture becomes measurable?**

**Security management with a future: part 2**

Article UA

september 2011

Annemie De Boye, CEO Modus Operandi and senior security consultant Robrechts & Thienpont
Paul Robrechts, CEO Robrechts & Thienpont

**The H-factor**

In the previous article we described how the "security" theme increasingly evolves into a new paradigm to fundamentally address the specific issues surrounding man and his security systems. We called it the "commitment paradigm". Crucial here is the idea that man as a key factor must be integrally involved in the system and the values ​​of the company. In this article we fully develop the concept from a security point of view, but the word "security" can be perfectly replaced with “safety”: both approaches are almost identical.

In security issues the **human factor** is present anywhere and anytime. Therefore it is not sufficient to optimize a company's security policies and technologies: when human security behavior is overlooked, we neglect an important and often weak link in the security chain. This is eg the case when employees are not aware of security risks. Or when security is regarded as an important issue, but not as a responsibility of each individual. If security procedures are not part of the daily routine, the "security" issue, for most members of the company, remains an abstract and far-away theme.

The security developments in the last decade have therefore significantly focused on this human factor. Through education and training companies try to teach executive staff not only knowledge and skills related to security, but they also aim to increase security *awareness* among their employees.

Several scientific studies as well as practical experience show that merely increasing the security awareness through procedures, education and training, is not necessarily sufficient to also create a security *culture*. Often there is a discrepancy between the theory that people proclaim (espoused theory) and their behavior in practice (theory in use)[[1]](#footnote-1). A well-developed security culture assumes that all members of the organization intentionally, consciously ànd consistently deal with security. This means that security culture should be an inherent part of the overall corporate culture. If this is not the case, then, the introduction of security measures can be compromised by the prevailing organizational culture and social imperatives among employees. The security manager must therefore always wonder if the security policy fits into the organizational culture and vice versa[[2]](#footnote-2).

According to a survey among security managers in medium and large-scale companies by Bon Bini Research, a well-developed security culture for many companies remains just a vaguely pursued goal. The biggest stumbling block for security by these leaders is defined as "a lack of adequate resources such as time, personnel or money." The second difficulty they call "constantly having to drag colleagues because of a lack of security consciousness." The other problems are named as "a lack of expertise," "the lack of a security culture," "lack of management cooperation" and "a lack of technical support and sensitivity to security concerns."[[3]](#footnote-3)

An ideal security culture within the company is a culture "where employees feel co-ownership within a fixed set of security principles, in which they are constantly trained in good security practices, and in which they also feel responsible for what they undertake.[[4]](#footnote-4)" An optimal security culture thus includes people, processes and technology. From this point of view, security is not an exclusive problem of the workplace, but also a task of general management[[5]](#footnote-5)..

The development of a security culture within a company is often related to a specific event. The most famous example in the security field comes from the French company DuPont. The motivation of the explosives company to make safety and security priority corporate objectives is nearly 200 years old. In 1818, shortly after founding the company, a gunpowder mill exploded. Forty people were killed and the gunpowder mill was destroyed. The owner, whose wife was severely wounded, realized that the survival of his business depended on the prevention of similar accidents. To get management to become more involved in the security issues, they were obliged to live on the company premises.

The concept of security culture came specifically in the spotlights with the report of the International Atomic Energy Agency (IAEA) on the disaster in Chernobyl (1986). This report states that security culture is the collection of characters and attitudes in organizations and individuals. These must ensure that, with the highest priority, nuclear safety and security issues get the necessary attention. That’s what, in the Chernobyl nuclear power plant, was missing . The accident, according to the IAEA, was partly caused by poor safety culture. This observation has led to the development of safety and security culture dynamics and to recommendations to improve these[[6]](#footnote-6).

**Security Culture and The Catalyst**

If we state that security culture must be embedded in or at least should be congruent with the prevailing organizational culture, the necessity naturally arises to define the concept of "culture". There is no unambiguous definition of security culture. The definitions of security culture found in specific literature are generally confined to the operation of high risk companies, as in the field of nuclear power plants or the (petro-) chemical industry.

For the sake of this article, we consider culture as "that which, within the company, is considered as good[[7]](#footnote-7)", referring to"a set of norms and values​​, assumptions, interpretations and practices that are characteristic for the organization. [[8]](#footnote-8)" This culture includes both visible and explicit elements, and invisible and implicit elements.

Security culture does not arise from coincidences. The adequate integration of security in the overall business process requires a delicate balancing act between three components: management support, management of security at the level of the security manager, and the security practices of each member of the company individually. A clear view on the interpretation of the security policy on each of these levels is an absolute prerequisite to improve the process, since they are highly interconnected and constantly influence each other.

To create a clear picture of the interaction between these components, Robrechts & Thienpont developed the Security Culture Circle or The Catalyst. The circular presentation of the dynamics surrounding security emphasizes that developing a security culture is not a stepwise process, but a continuous search for balance in which the various actors within the organization constantly influence each other and set each other in motion.



Thus, the Security Culture Circle acts as a catalyst for sustainable change. The model approaches the organization from a global, integrated perspective, working simultaneously on the three components. The evolution towards a stronger security culture consists of multiple movements at different levels, each in turn inciting new security change management processes. This continuous process works to the benefit of all stakeholders in the company: employees, managers, customers and business associates.

**The Maturity Scale : The Security Maturity Model**

Above we described how security is evolving to be an integral element of the business process, fully in service of the core business. Contributing to the corporate objectives becomes an essential part of security management. If we succeed in identifying and picturing the organizational culture, and particularly the security culture within an organization, then we can grant the company a position on the so-called maturity scale. This scale indicates to what extent the intended evolution to a full role and positioning of security within the organization has already been achieved.

Through questionnaires and interviews, the organization can be evaluated on the three levels of The Catalyst: management support, security management and implementation at the workplace, the security practices. Each level is then scored on the three primary elements that influence human behavior : knowledge, skills and commitment. Indeed, cognition, competences ànd attitude will be three necessary conditions for an effective security culture to arise.

The result of this analysis is a matrix containing 9 cells. Each cell receives a score on the Security Maturity scale from the lowest score "denial" to the highest score "strategi”. Thus, for each level of the company (management, security manager and executive staff), we can determine to what extent, given their knowledge, expertise and commitment, they may or may not contribute to a positive security climate.

If we then consider all cells together, we obtain an overall score for the entire company. This gives us a picture of the situation “as is”, a scan in which not only the possible discrepancies between certain levels of the company are demonstrated, but that also gives a rough estimate of the company’s position on the general culture scale.

**knowledge**

 **skills**

**commitment**

**cognitive**

**competence**

**attitude**

**management**

**support**

**security**

**management**

**security**

**practices**

**Denial**

Organizations in the denial stage deny all security risks. There is little or no attention to security, and the people in the workplace are not involved. Security behavior or security policy are not an issue.

**Reactive**

Companies situated in the reactive phase operate ad hoc and only react to specific incidents. Individual employees are approached with separate procedures, but only with the intention of controlling the damage. Skills and knowledge about security are developed based on actual events. Security is used as a means of symptom control.

*Within the above two levels there is no question of a structural or preventive security policy. The security theme only gets attention when specific problems or incidents occur. Organizations on either of these levels are approaching security from a simply reactive perspective.

From the third level on, however, the approach becomes more and more proactive. Organizations that are situated on one of the following three levels are looking at security as a risk that is to be addressed structurally at the company level as well as from a preventive point of view.*

**Systematic**

Companies that handle a systematic approach, implement their security policy both at the level of the management and at the level of the subgroups. Security, here, is approached in the same systematic way as the other business risks. The company therefore has the necessary systems to manage these risks. Security behavior is driven by personal motivation. The staff are generally trained on the collective system indicators. The function of the security manager remains essentially operational and close to the primary process.

**Proactive**

When an organization is situated on the proactive level, not only the executive staff but also the management and the organization as a whole are aware of the importance of security. Security is proactively integrated into the overall business process. Security trainings are differentiated and adapted to individual needs. Security increasingly becomes a part of the business management, and the security manager gets a more strategic role and position.

**Strategic**

At the highest level, the strategic one, the entire organization from the shareholders and stakeholders on to the operational level is aware of the importance of security. The security policy is regarded as an obvious theme, and security behavior is an automatism for everyone. Security is fully integrated into the business process and belongs to the core values ​​of the company. Not only the security manager but also the entire top management display these values​​.

**The new paradigm : aiming for a strategic approach to security**

It is clear that, within the new "commitment paradigm", this strategic level becomes the ultimate goal. Here, getting the entire organization involved in the security policy has become a top management responsibility. A company that approaches security in a strategic way is characterized by the following elements:

- Security has an important position within the business strategy, and interventions in the security field are part of the key values ​​of the company. Managers therefore give broader and longer-term perspectives to security, they lead the way, and can **convince** people of the importance and need for security. This ultimate strategic approach to security is characterized by a visible effort at the senior management level and board of directors level.

- Moreover, the management stays **in touch** with the operational process by being present on the work floor, talk with staff and receive feedback on the security policy. They are hereby aware of their exemplary functions and thus explicitly comply to all security procedures themselves.

- Within this strategic framework the organization has a **documented policy** that clearly states the company's commitment in the security field. It was developed through extensive consultation and is explicitly communicated to all employees and other potential stakeholders. A clear commitment from top management is required to continuously assess the security performances.

- Of course, the necessary **resources** to support the security policy are provided: there are sufficient budgets for training, and relevant resources and experts in the security field are present. Part of management time is spent on security. The means are provided to ensure that the improvements in the security domain are profitable.

- Employees **participate** in the security activities and fully cooperate with employers for safe and secure workplaces. With the operational staff, the new and established policies, practices and performances in the field of security are systematically discussed. The goals and objectives associated with the security policy are democratically discussed to ensure continuous improvements in the security field, and these are regularly reviewed. Every single employee is aware of his responsibility regarding the safety and security of those they are entrusted, of themselves, of any others with whom they work and of anyone else who visits the site.

- Continuous **training programs** ultimately ensure that employees remain aware of security issues, and of their own responsibility regarding it. The trainings also ensure that employees are capable of performing the tasks imposed upon them ; their professional skills are assessed and refreshment courses are systematically provided. [[9]](#footnote-9)

Security culture thus fits within a high-reliability organization. To achieve this, management disposes of the right information, operational levels report on relevant security issues and the organization is able to adapt to new situations and learn from its own experiences. Security in the workplace is also related to issues of mutual collegiality: the willingness to report unsafe behavior to and from each other and thus safeguard people and organization from accidents. An important condition is that it is a 'blame free' organization, with clear boundaries between acceptable and unacceptable behavior. [[10]](#footnote-10)

**Security culture matrix : a useful tool**

Measuring the security culture within a company is not only useful to launch a culture change process. The measurement itself too has a positive impact. A Norwegian study shows that the measurement of security awareness and of compliance with security best practices, can increase the level of security practices within organizations, resulting in fewer security incidents related to carelessness or neglect. Employees in such an environment took more responsibility for securing physical and data materials, and they took up a more active role in discovering and reporting incidents[[11]](#footnote-11)

The measurements further improve not only the involvement of employees in the security culture, but they can also be used to promote a company-wide vigilance by supervisors and line managers in the regular analysis of the security measurements involved.

The mere consciousness of employees and managers that security culture figures are collected on a regular basis and that these are viewed by senior management can also contribute substantially to compliance with the security policy.

**Conclusion : the challenge**

"The total sum of figures considering security technologies, processes and behavior can give us a clearer perspective on the security situation of the company”, security experts say. However, creating an instrument to measure security culture does not generate a generally valid and universally applicable toolbox. Every organization is unique, and the instruments that measure behavior should be carefully adjusted to capture the relevant conduct and the relevant processes." [[12]](#footnote-12)

Therefore, there is no such thing as a universal audit schedule that is adequate for all companies. Each organization is different, and thus each audit will have to be tailor-made: fitting the client. A standardized questionnaire to get started with - a quick scan as it were- can nevertheless provide useful information for launching the tailor-made audit. This scan allows us to allocate companies a position on the maturity scale, giving them a clear picture of their position within a generally applicable frame of reference. The scan also shows which segments of the organization are the weakest areas, and thus to which ones priority attention will have to be given. This way, not only the subsequent audit gets proper direction and depth, but at the same time the impetus is given to initiate the necessary change processes...

"Working in a safe and secure environment remains a challenge, every day. What is important today is how the overall organization integrates security and safety into her daily thoughts and actions. Security as a choice, as a value and as a culture.[[13]](#footnote-13)" Taking into account the specific risks, you therefore have the choice to determine where your company intends to position itself on the maturity ladder, and how important security is for your organization.

1. “Veiligheidscultuur an de werking van het veiligheidsbeheerssysteem bij BRZO-bedrijven”, Ing. Menno Meems and Jan ten Hove. [↑](#footnote-ref-1)
2. “Security culture : the missing link?”, by Jaak Colson at the R&T congres “Security meets the future”, on march 15th, 2011. [↑](#footnote-ref-2)
3. Bon Bini, “Veiligheids- en Welzijnsenquête 2011 : de resultaten” in Veiligheidsnieuws, September 2011. [↑](#footnote-ref-3)
4. “Measuring and Evaluating an Effective Security Culture”, white paper, Cisco Systems inc. [↑](#footnote-ref-4)
5. Paul Robrechts, part 1. [↑](#footnote-ref-5)
6. ir E. van der Reijden, August 2000, Master of Crisis and Disaster Management, "Security culture: what can the fire department, in case of repressive action, learn from the chemical industry?” [↑](#footnote-ref-6)
7. “Security culture : the missing link?” by Jaak Colson at the Robrechts & Thienpont congres “Security meets the future” march 15th, 2011 [↑](#footnote-ref-7)
8. Definition Quinn en Cameron [↑](#footnote-ref-8)
9. All these characteristics represent specific considerations as described in the contest program for the "Prize of the High Council for Prevention and Protection at Work." Here, the risks to both security ànd safety are treated equally. [↑](#footnote-ref-9)
10. ir E. van der Reijden august 2000,Master of Crisis and Disaster Management, “Veiligheidscultuur: wat kan de brandweer voor het repressief optreden leren van de chemische industrie?” [↑](#footnote-ref-10)
11. “Measuring and Evaluating an Effective Security Culture”, white paper, Cisco Systems inc. [↑](#footnote-ref-11)
12. Measuring and Evaluating an Effective Security Culture”, white paper, Cisco Systems inc. [↑](#footnote-ref-12)
13. Bon Bini, “Veiligheids- en Welzijnsenquête 2011 : de resultaten” in Veiligheidsnieuws, september 2011 [↑](#footnote-ref-13)